

Having your phone call redirected when calling the number on the back of a credit or debit card is a serious indicator of a call forwarding scam or compromised phone settings. Fraudsters can set up malicious call forwarding, causing your outbound call to a bank to be intercepted by a third party pretending to be customer service.

Here is a breakdown of what is happening, how it works, and how to fix it based on the search results. What is Happening?

- **Intercepted Calls:** You dial the legitimate bank number, but the call is rerouted to a scammer who answers as if they are the bank.
- **Purpose:** The goal is to get you to divulge personal information like PINs, passwords, or card numbers.
- **Method:** Scammers use social engineering to trick carriers into enabling call forwarding, or they use malicious software/codes on your phone to turn it on.
-

How to Detect and Fix the Issue

If you suspect your calls are being redirected, take these actions immediately:

1. **Use Deactivation Codes:** Dial **##002#** or **#67#** on your phone keypad to deactivate all call forwarding.
2. **Check Phone Settings:** Go to your phone's "Call Settings" > "Call Forwarding" and ensure it is turned off.
3. **Perform a Factory Reset:** If the redirect persists, some users have reported that a factory reset of the phone removes the malicious redirect.
4. **Contact Your Carrier:** Call your mobile service provider to ask them to check for unauthorized "Remote Call Forwarding" on your account.
5. **Remove/Reinsert SIM:** If codes fail, try removing and reinserting your SIM card or toggling airplane mode to reset the network connection.
- 5.

Safety Measures

- **Do Not Trust "Saved" Numbers:** Even if the number is on the card, verify it against the official website if something seems off.
- **Listen for Clues:** If the person answering has an accent not typical for the bank or asks for highly sensitive data immediately (e.g., CVV), hang up.
- **Initiate, Don't Receive:** Only give out sensitive information on calls you initiated.
- **Check Phone Records:** Review your phone records to see what number was actually dialed.
-

Disclaimer: If you have already given information to a suspect, contact your bank immediately through a different, trusted device and freeze your account.